Secure Transmission Design for Cognitive Radio Networks with Poisson Distributed Eavesdroppers

Xiaoming Xu, *Student Member, IEEE,* Biao He, *Student Member, IEEE,* Weiwei Yang, *Member, IEEE,* Xiangyun Zhou, *Member, IEEE,* and Yueming Cai, *Senior Member, IEEE*

***Abstract*—In this paper, we study physical layer security in an underlay cognitive radio (CR) network. We consider the problem of secure communication between a secondary transmitter-receiver pair in the presence of randomly distributed eavesdroppers under an interference constraint set by the primary user. For different channel knowledge assumptions at the transmitter, we design four transmission protocols to achieve the secure transmission in the CR network. We give a comprehensive performance analysis for each protocol in terms of transmission delay, security, reliability, and the overall secrecy throughput. Furthermore, we determine the optimal design parameter for each transmission protocol by solving the optimization problem of maximizing the secrecy throughput subject to both security and reliability constraints. Numerical results illustrate the performance comparison between different transmission protocols.**

***Index Terms*—Physical layer security, cognitive radio networks, on-off transmission, secrecy guard zone.**

I. Introduction

A. Background and Motivation

With the rapid adoption of wireless devices, there is an unprecedented growth in the demand for radio spectrum. To address the conflict between spectrum scarcity and spectrum underutilization, cognitive radio (CR) [1–3] has been regarded as a promising technology to solve the problem of inefficient spectrum usage. In CR networks, unlicensed secondary users (SUs) are allowed to access the spectrum of licensed primary users (PUs) with the requirement of not interfering the PUs. Generally, there exist two paradigms of CR networks classified by the spectrum access strategy: i) overlay CR [4, 5] and ii) underlay CR [6, 7]. For the overlay CR, the SUs first adopt spectrum sensing techniques to identify the licensed spectrum hole, and then transmit data over the detected spectrum holes. For the underlay CR, the SUs simultaneously utilize the licensed spectrum while guaranteeing the interference at the PU not beyond the acceptable threshold.

Allowing the spectrum sharing in the CR network is not without drawbacks. The coexistence of licensed and unlicensed users in the same network makes the data transmissions vulnerable to security attacks [8]. To address this concern, innovative security technologies have been proposed for CR networks [8]. As a complement to the traditional cryptographic techniques [9], physical layer security (PLS) has been widely studied [10] [11] to secure the wireless transmissions by exploiting the fading characteristics of wireless channels.

To the best of authors' knowledge, the current research on PLS in CR networks assumed that either the channel state information (CSI) of eavesdropping channel is perfectly known or there are a small number of eavesdroppers at known locations. In practical scenarios, a passive eavesdropper would not reveal its CSI or location information to the legitimate communication nodes, and hence such assumptions are not always valid. Taking into account potentially a large number of eavesdroppers inside the network at random and possibly changing locations (due to mobility), a common analytical approach is to model the location set of eavesdroppers to be a stochastic process following some distribution [12–14]. For the secure communication in CR networks, the consideration of randomly distributed eavesdroppers has been rarely discussed in CR networks.

B. Our Approach and Contribution

In this paper, we study the problem of achieving PLS in an underlay CR network where a secondary transmitter (SU-Tx) sends confidential information to a secondary receiver (SU-Rx) over a quasi-static Rayleigh fading channel in the present of multiple eavesdroppers. The location set of the eavesdroppers is modeled as a homogeneous Poisson point process (HPPP).[1] We consider different transmission protocols for the SU-Tx to achieve secure communication while guaranteeing the instantaneous interference to the primary receiver (PU-Rx) not beyond a given threshold. To satisfy the interference constraint, the transmit power at the SU-Tx is carefully adjusted, which is determined by the instantaneous channel condition from the SU-Tx to the PU-Rx.

We consider four transmission protocols to achieve the secure transmission in the CR network: the full activity protocol, the secrecy guard zone protocol, the threshold-based protocol and the hybrid protocol. These four different protocols are suitable for the scenarios with different assumptions on the channel knowledge of the SU-Tx and the location knowledge about the eavesdroppers. Specifically, the full activity protocol is for the scenario where the SU-Tx does not have any knowledge about the CSI of its receiver and the location

This work was supported by the Natural Science Foundation of China under Project 61371122, Project 61471393, and the Australian Research Council under Discovery Project Grant DP150103905.

X. Xu, W. Yang and Y. Cai are with College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China (e-mail: xiaomingxu.plaust@gmail.com, wwyang1981@163.com, caiym@vip.sina.com).

B. He and X. Zhou are with the Research School of Engineering, Australian National University, Canberra, ACT 0200, Australia (e-mail: biao.he@anu.edu.au, xiangyun.zhou@anu.edu.au).

[1] HPPP has been widely adopted to model the eavesdropper locations in the existing literature, e.g., [12, 13, 15].

information of the eavesdroppers. The secrecy guard zone protocol is for the scenario where the SU-Tx can detect the existence of eavesdroppers in its vicinity, i.e., a circular guard zone of radius r. The SU-Tx suspends the transmissions when eavesdropper(s) are detected inside the guard zone. The threshold-based protocol is for the scenario where the SU-Tx can obtain a one-bit feedback about the SU-Tx's instantaneous channel gain. The SU-Tx suspends the transmissions when the channel gain is worse than some threshold μ. Finally, the hybrid protocol includes both the secrecy guard zone and the threshold-based transmissions, hence, is expected to have the best performance.

For each transmission protocol, we evaluate various quality-of-service measures by studying performance metrics related to transmission delay, security and reliability. Specifically, we use outage-based metrics which are suitable for quasi-static fading channels. Instead of adopting a widely-used outage probability of secrecy capacity [16] which does not distinguish between outages due to suspended transmission (i.e., delay), information leakage to eavesdroppers (i.e., security) and unreliable reception at the intended receiver (i.e., reliability), we use separate outage metrics for each type of quality of service. We also define an outage metric called transmission secrecy outage probability (TSOP) that comprehensively evaluates the security and reliability performance in order to tell the probability of having a secure and reliable transmission. The tradeoff between security and reliability is also captured by the TSOP. Finally, the overall performance of each protocol is measured by the secrecy throughput defined as the achievable average rate of secure and reliable transmissions.

We further optimize the design of transmission protocols based on the derived outage probabilities and secrecy throughput expressions. To this end, we study the optimization problem of achieving the maximal secrecy throughput with given security and reliability outage constraints. We first study the feasible security and reliability constraints for each transmission protocol, under which a non-zero secrecy throughput is achievable. We then obtain the closed-form solutions of the optimal guard zone's radius r and/or the optimal SNR-threshold μ that maximize the secrecy throughput for the corresponding transmission protocols. Our results show that the secrecy guard zone protocol is preferred when the security constraint is stringent while the threshold-based protocol is preferred when the reliability constraint is stringent.

The remainder of this paper is organized as follows. Section II discusses the related work. Section III gives the channel model and performance metrics. Section IV introduces the four transmission protocols. Sections V and VI evaluate and optimize the transmission protocols, respectively. Section VII presents the numerical results. Finally, Section VIII concludes the paper.

II. Related Work

Underlay CR communications [6, 7] has received a lot of attention as a promising paradigm to improve spectrum usage efficiency, e.g., [17–19] focusing on the performance analysis and [20–24] investigating the network design. In recent years, there has been increasing interest in the security issue of CR networks, due to the rapid growing amount of private and sensitive data transmitted in wireless networks. From an information-theoretic perspective, the performance of PLS in CR networks was studied in, e.g., [25–29]. The ergodic secrecy capacity for the CR network was evaluated in [25, 26] with the consideration of fast fading channels where the encoded messages are assumed to span sufficient channel realizations to capture the ergodic features of the fading channel. Considering the slow fading channels, the secrecy performance of the CR network was evaluated in [27] by the outage-based formulation. The secrecy throughput scaling laws were investigated in [28, 29]. More recently, various signal processing techniques and system design protocols were proposed to improve the secrecy performance of the CR networks. For the multi-antenna CR network, beamforming designs and cooperative jamming techniques were studied in [30–32]. For the CR network with multiple SUs, the user scheduling scheme for improving the security level of cognitive transmissions was proposed in [33]. Furthermore, the CR network with decode and forward relays was studied in [34] where the optimal relay selection scheme to minimize the secrecy outage probability was proposed.

As mentioned in Section I-A, the consideration of randomly distributed eavesdroppers has been rarely discussed in CR networks. However, the randomly distributed eavesdroppers are often considered in the study on PLS in large-scale wireless networks using tools from stochastic geometry [35]. The network model based upon stochastic geometry allows us to study the probabilistic network behaviors and corresponding performance metrics [36–38]. In particular, the location set of the randomly distributed eavesdroppers is often modeled by the HPPP, e.g., [12, 14, 15, 39–41]. The HPPP-based model not only provides tractable closed-form results but also describes the randomness of eavesdropper locations in practical scenarios [41]. Specifically, Goel *et al.* [14] introduced a secrecy graph model based on the HPPP to capture the uncertainty in eavesdropper locations at the network level. Pinto *et al.* [12] proposed the *Poisson iS*-graph to study the secrecy connectivity of large scale network. Zhou *et al.* [15] investigated the secrecy transmission capacity of the wireless network. Furthermore, the scaling laws for secrecy capacity were investigated in [39–41]. For the secure communication in CR networks, the consideration of randomly distributed eavesdroppers has been studied in [42, 43], in which Shu *et al.* considered that the message to the PU is confidential and derived the secrecy capacity in the presence of randomly distributed eavesdroppers whose location set is modeled as a HPPP. However, the work in [42, 43] only considered a simplified channel model consisting of the pass loss effect only, while the fading effect is not considered. It is important to note that the performance of secure communication is very different between a fading and a non-fading scenario. Furthermore, the presence of fading can be smartly utilized to achieve a better security performance.

It is worth mentioning that the literature review in this section focuses on only the most closely related work in the areas of CR networks, PLS in CR networks, and PLS in

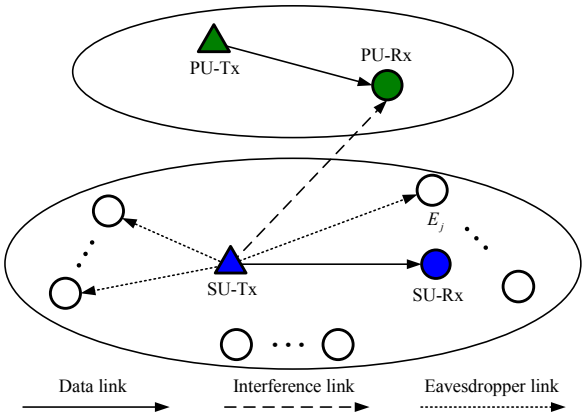


Fig. 1. Illustration of a cognitive radio network with a Poisson field of eavesdroppers.

large-scale wireless networks. Due to the rapid development of wireless technology and the increasing demand of secure communications, there also exists many other interesting studies on the current and next generation of wireless networks and communication security, e.g., [44–56].

III. System Model

A. Channel Model

As shown in Figure 1, we consider an underlay CR network that consists of a primary transmitter-receiver pair and a secondary transmitter-receiver pair. The SU-Tx sends confidential messages to the SU-Rx in the present of multiple movable eavesdroppers, which are denoted by $\{E_j|j=1,2,\cdots\}$. The primary network allows the secondary network to share the spectrum by underlay method, and requires that the instantaneous interference power at PU-Rx from SU-Tx is lower than a threshold, denoted by I_0.

We assume that the eavesdroppers are randomly distributed in the network. The location set of the eavesdroppers, denoted by Φ_E, is modeled as a HPPP with density λ_E. Different from the deterministic model, the spatial HPPP introduces total randomness for the node deployment, and only the node density variable is required to characterize this stochastic process. In addition, the randomness introduced by the HPPP-based model has the advantage of being tractable in performance analysis, since it often leads to closed-form results on statistical analysis for signal attenuation laws [57]. By adopting the PPP-based topology for wireless networks with randomly distributed nodes, important results on connectivity, coverage, and throughput have been successfully derived in [36, 58, 59].

In this work, we assume that all communication nodes have a single antenna and the wireless communication channel is modeled as a path-loss plus quasi-static Rayleigh fading channel. Denote the transmitter power at SU-Tx as P. Then, the received signal to noise ratios (SNRs) at the SU-Rx and eavesdropper E_j are given by

$$\gamma_D = \frac{P}{\sigma_D^2}\left|h_{SD}\right|^2 d_{SD}^{-\alpha} \tag{1}$$

and

$$\gamma_{E_j} = \frac{P}{\sigma_{E_j}^2}\left|h_{SE_j}\right|^2 d_{SE_j}^{-\alpha}, \tag{2}$$

respectively, where $\alpha \geq 2$ denotes the path loss exponent, d_{SD} and d_{SE_j} denote the distance from SU-Tx to SU-Rx and the distance from SU-Tx to E_j, respectively, σ_D^2 and $\sigma_{E_j}^2$ denote additive white Gaussian noise (AWGN) variances at SU-Rx and E_j, respectively, with $\sigma_D^2 = \sigma_{E_j}^2 = \sigma^2$. In addition, h_{SD} and h_{SE_j} denote the channel coefficients for the channel from SU-Tx to SU-Rx and the channel from SU-Tx to E_j, respectively, which are modeled as complex Gaussian variables with zero mean and unit variance, i.e., $\mathcal{CN}(0,1)$. We further assume that the interferences from PU-Tx at the SU-Rx and the eavesdroppers are neglectable. We highlight that such an assumption is widely adopted in the literature studying CR networks, e.g., [27, 33, 60–62]. A practical example that approximates this occurrence is the scenario where the PU-Tx is located far away from the terminals in the secondary network [61].

We assume that the receiver side (including PU-Rx, SU-Rx and the eavesdroppers) has the perfect CSI, while the availability of CSI at the transmitter-side is different between PU-Rx and SU-Rx due to the different capabilities of the communication terminals. We consider a scenario where the PU-Rx is a cellular base station which is capable of instantaneous CSI feedback to both PT-Tx and SU-Tx, while the SU-Rx is not capable of full CSI feedback. Specifically, the PU-Rx feeds back to the SU-Tx with the instantaneous channel gain, denoted by $|h_{SP}|^2$, to enable the SU-Tx to adjust its transmit power to satisfy the interference constraint [17–19].[2] Although the SU-Rx is not capable of full CSI feedback, we consider the possibility of a low-complexity feedback scheme in which the SU-Rx uses one bit to inform SU-Tx about its channel condition. The eavesdroppers are totally passive, and hence their CSI is not revealed to SU-Tx.

To satisfy the instantaneous interference constraint, I_0, the SU-Tx adjusts the transmit power to

$$P = \frac{I_0}{\left|h_{SP}\right|^2 d_{SP}^{-\alpha}}\mathbf{1}_{(\text{condition})}, \tag{3}$$

where d_{SP} denotes the distance from SU-Tx to PU-Rx, and $h_{SP} \sim \mathcal{CN}(0,1)$. The $\mathbf{1}_{(\text{condition})}$ in (3) denotes an indicator function for whether the transmission is "on" or "off" at SU-Tx, which is given by

$$\mathbf{1}_{(\text{condition})} = \begin{cases} 1, & \text{if the condition holds} \\ 0, & \text{otherwise,} \end{cases} \tag{4}$$

where the condition depends on the specifical transmission protocol, and will be detailed later in Sections IV. Note that having such an "on-off" transmission strategy can effectively improve the security and/or reliability performance, as will be shown in Sections V.

[2]This can be achieved through a spectrum-band manager that mediates between the licensed and unlicensed users [63]. However, it is worth noting that, for certain scenarios, obtaining the interference channel power gains may be challenging. For these cases, our results serve as the bounds for the performance of the considered network.

For a robust analysis, we consider that all eavesdroppers can collude and exchange information. Thus, the multiple eavesdroppers can be regarded as a single eavesdropper, E_{joint}, with multiple distributed antennas, and the equivalent received SNR at the E_{joint} is given by

$$\gamma_E = \frac{P}{\sigma^2} \sum\nolimits_{E_j \in \Phi_E} \left|h_{SE_j}\right|^2 d_{SE_j}^{-\alpha}. \tag{5}$$

From (1) and (5), we note that γ_D and γ_E have the same power variable P, which makes them correlated with each other. For convenience, we define $Z_{\Phi_E} = \sum_{E_j \in \Phi_E} \left|h_{SE_j}\right|^2 d_{SE_j}^{-\alpha}$ in the following analysis.

B. Secure Encoding

The SU-Tx uses the widely-adopted wiretap code [64] to encode the confidential messages. Let $\mathbb{C}\left(R_B, R_S\right)$ denote the set of all possible Wyner codes, where R_B is the codeword transmission rate and R_S is the confidential information rate with $R_B > R_S$. The rate difference $R_B - R_S$ reflects the cost of securing the message against eavesdropping. We assume that the encoding rates have already been designed, and hence R_B and R_S are fixed.[3] Such a fixed-rate transmission scheme is suitable for practical applications requiring low complexity, e.g., video streams in multimedia.

C. Outage Probability Metrics

In the following, we detail the outage definitions for characterizing the transmission delay, the security performance and the reliability performance of the network. Moreover, we propose a new probability metric to comprehensively evaluate the joint performance of security and reliability.

1) TP: Since the transmission may not always happen at SU-Tx depending on the transmission protocol, there exists a probability of transmission referred to as TP, which is given by

$$p_{\text{tx}} = \mathbb{P}\left(\mathbf{1}_{(\text{condition})} = 1\right), \tag{6}$$

where $\mathbb{P}(\cdot)$ denotes the probability measure. We adopt the probability of transmission as a measure of the performance of transmission delay [65].

2) SOP and COP: With the fixed-rate wiretap code, there exist two kinds of outage events [65, 66]: secrecy outage event and connection outage event. The secrecy outage event happens when the perfect secrecy of the message cannot be guaranteed, and the probability of the secrecy outage referred to as SOP is given by [65]

$$p_{\text{so}} = \mathbb{P}\left(C_E > R_B - R_S \middle| \mathbf{1}_{(\text{condition})} = 1\right), \tag{7}$$

where $C_E = \log\left(1+\gamma_E\right)$ denotes the channel capacity of E_{joint}. The connection outage event happens when the message cannot be decoded at the intended receiver without error, and the probability of the connection outage referred to as COP is given by

$$p_{\text{co}} = \mathbb{P}\left(C_B < R_B \middle| \mathbf{1}_{(\text{condition})} = 1\right), \tag{8}$$

[3]The design of rate parameters is beyond the scope of this work.

where $C_B = \log\left(1+\gamma_D\right)$ denotes the channel capacity of the secondary link. In this work, we adopt the SOP as a measure of the security performance and the COP as a measure of the reliability performance.

3) TSOP: From (7) and (8), we note that the security and reliability become correlated in the considered CR network due to the correlation between γ_D and γ_E. This is actually different from the case in most of the non-cognitive scenarios, e.g., [15, 66, 67]. Therefore, it is necessary to comprehensively study the joint performance of the security and the reliability. To this end, we propose a new outage performance metric, namely transmission secrecy outage probability (TSOP). The TSOP characterizes the probability that either secrecy outage or connection outage happens, which is given by

$$p_{\text{tso}} = 1 - \mathbb{P}\left(C_E \le R_B - R_S, C_B \ge R_B \middle| \mathbf{1}_{(\text{condition})} = 1\right). \tag{9}$$

Remark 1: Comparing the expressions of p_{so}, p_{co} and p_{tso} in (7), (8) and (9), we note that the TSOP takes the mutual correlation between the SOP and the COP into account. For the special case that SOP and COP are independent,[4] the TSOP can be further derived as

$$p_{\text{tso}} = 1 - \left(1 - p_{\text{co}}\right)\left(1 - p_{\text{so}}\right). \tag{10}$$

Remark 2: The proposed TSOP characterizes the joint security and reliability performance. In fact, a similar concept of jointly measuring security and reliability performance can be found in another widely-adopted outage probability definition, i.e., $p_{\text{out}} = \mathbb{P}\left(C_S < R_S\right)$ [16], where C_S denotes the secrecy capacity. Compared with the expression of p_{out}, the proposed TSOP takes into account the system design parameters, such as the rate of the transmitted codewords as well as the condition under which message transmission happens.

D. Secrecy Throughput

The overall performance of the system is measured by the secrecy throughput taking into account the transmission delay, the security performance and the reliability performance together. The secrecy throughput is given by

$$\eta = p_{\text{tx}}\left(1 - p_{\text{tso}}\right) R_S, \tag{11}$$

where p_{tx} is the TP in (6) and p_{tso} is the TSOP in (9). As mentioned before, p_{tx} quantizes the transmission delay performance and p_{tso} quantizes the joint security and reliability performance. As such, the secrecy throughput in (11) quantizes the average secrecy rate at which the messages are securely and reliably transmitted to SU-Rx.

It is worth mentioning that the secrecy throughput in (11) is different from the throughput definition in [65] and [66]. In [65] and [66], the throughput is formulated as

$$\eta = p_{\text{tx}}\left(1 - p_{\text{co}}\right) R_S, \tag{12}$$

which quantizes the average secrecy rate at which the messages are reliably transmitted to SU-Rx. We find that the throughput expression in (12) does not reflect whether the

[4]When the transmit power is fixed in cognitive or non-cognitive networks, the SOP and COP usually are independent [15, 66, 67].

transmission is secure, and hence it is proper to use the secrecy throughput expression in (11) for characterizing the *overall* performance of the transmission.

IV. Secure Transmission Protocols

For the considered CR network as described in Section III, there are four possible cases of channel knowledge assumptions at the SU-Tx, which are detailed as follows: 1) SU-Tx does not know any information about the channel condition to the SU-Rx and does not know any information about the eavesdropper locations; 2) SU-Tx does not know any information about the channel condition to the SU-Rx but can detect the existence of eavesdroppers in its vicinity; 3) SU-Rx has the one-bit feedback about the channel condition to the SU-Rx but does not know any information about the eavesdropper locations; 4) SU-Rx has the one-bit feedback about the channel condition to the SU-Rx and can detect the existence of eavesdroppers in its vicinity. These four cases complete the possible channel knowledge assumptions at the SU-Tx for the considered CR network. Accordingly, we design four secure transmission protocols which are full activity protocol, secrecy guard zone protocol, threshold-based protocol and hybrid protocol. The details of each protocol are given in the following subsections.

A. Full Activity Protocol

For the full activity protocol, the SU-Tx can neither obtain the one-bit feedback from the SU-Rx nor detect the existence of eavesdroppers in its vicinity. Therefore, the SU-Tx keeps sending the confidential information to the SU-Rx all the time while satisfying the power constraints. This protocol is the simplest protocol amongst the four transmission protocols. Since the BS is always active, the indicator function in (4) is always equal to one, and the SNRs at the SU-Rx and the eavesdropper E_{joint} are given by

$$\gamma_D = \frac{I_0|h_{SD}|^2 d_{SD}^{-\alpha}}{\sigma^2|h_{SP}|^2 d_{SP}^{-\alpha}} \tag{13}$$

and

$$\gamma_E = \frac{I_0}{\sigma^2|h_{SP}|^2 d_{SP}^{-\alpha}} Z_{\Phi_E}, \tag{14}$$

respectively.

B. Secrecy Guard Zone Protocol

For the secrecy guard protocol, we consider the scenario where the SU-Tx is able to detect the existence of eavesdroppers within a finite range. As per the mechanism of secrecy guard zone [15, 68], we model the finite range around the SU-Tx as a secrecy guard circle $\mathcal{B}$ with radius r. The SU-Tx sends messages only when there is no eavesdropper detected inside the guard circle. Consequently, the SNRs at the SU-Rx and the eavesdropper E_{joint} under the secrecy guard zone protocol are given by

$$\gamma_D = \frac{I_0|h_{SD}|^2 d_{SD}^{-\alpha}}{\sigma^2|h_{SP}|^2 d_{SP}^{-\alpha}} \mathbf{1}_{(C_1)} \tag{15}$$

and

$$\gamma_E = \frac{I_0}{\sigma^2|h_{SP}|^2 d_{SP}^{-\alpha}} Z_{\Phi_E} \mathbf{1}_{(C_1)}, \tag{16}$$

respectively, where C_1 denotes the event that no eavesdropper is detected inside the secrecy guard zone, i.e., $\left\{C_1 : \forall E_j \in \Phi_E, d_{SE_j} > r\right\}$.

C. Threshold-Based Protocol

In the threshold-based protocol, we assume that the SU-Tx can obtain a one-bit feedback from the SU-Rx to enable a threshold-based on-off transmission. Specifically, the SU-Tx transmits only when the received SNR at SU-Rx is larger than a predetermined threshold μ. Otherwise, the SU-Tx suspends the transmission. To this end, the SU-Rx sends an instantaneous one-bit feedback to the SU-Tx for indicating whether the received SNR is larger the threshold μ. In such a protocol, the SNRs at the SU-Rx and the eavesdropper E_{joint} are given by

$$\gamma_D = \frac{I_0|h_{SD}|^2 d_{SD}^{-\alpha}}{\sigma^2|h_{SP}|^2 d_{SP}^{-\alpha}} \mathbf{1}_{(C_2)} \tag{17}$$

and

$$\gamma_E = \frac{I_0}{\sigma^2|h_{SP}|^2 d_{SP}^{-\alpha}} Z_{\Phi_E} \mathbf{1}_{(C_2)} \tag{18}$$

respectively, where C_2 denotes the event that the SNR at the SU-Rx is larger than μ, i.e., $\left\{C_2 : \frac{I_0|h_{SD}|^2 d_{SD}^{-\alpha}}{\sigma^2|h_{SP}|^2 d_{SP}^{-\alpha}} > \mu\right\}$.

D. Hybrid Protocol

In this protocol, we assume that the SU-Tx can not only detect the existence of eavesdroppers within the secrecy guard zone but also obtain the one-bit feedback from the SU-Rx, and hence, the SU-Tx adopts a *joint* secrecy guard zone and SNR threshold based transmission strategy. As the same to Section IV-B, we denote the secrecy guard zone as a circle $\mathcal{B}$ with radius r around the SU-Tx. As the same to Section IV-C, we denote the received SNR threshold as μ. The SU-Tx transmits only when both of the following two conditions are satisfied: 1) there is no eavesdropper in the secrecy guard zone around the SU-Tx; 2) the received SNR at SU-Rx is larger than the threshold μ. The AND rule is applied at the SU-Tx for determining whether to transmit, and the condition for transmission is given by $\left\{C_1 \& C_2 : \forall E_j \in \Phi_E, d_{SE_j} > r \text{ and } \frac{I_0|h_{SD}|^2 d_{SD}^{-\alpha}}{\sigma^2|h_{SP}|^2 d_{SP}^{-\alpha}} > \mu\right\}$. Then, the SNRs at the SU-Rx and the eavesdropper E_{joint} are given by

$$\gamma_D = \frac{I_0|h_{SD}|^2 d_{SD}^{-\alpha}}{\sigma^2|h_{SP}|^2 d_{SP}^{-\alpha}} \mathbf{1}_{(C_1 \& C_2)} \tag{19}$$

and

$$\gamma_E = \frac{I_0}{\sigma^2|h_{SP}|^2 d_{SP}^{-\alpha}} Z_{\Phi_E} \mathbf{1}_{(C_1 \& C_2)}, \tag{20}$$

respectively.

V. Performance Analysis

In this section, we derive the TP, the COP, the SOP and the TSOP for different transmission protocols, to characterize the transmission delay, the reliability, the security and the joint security and reliability performance, respectively.

A. Full Activity Protocol

In the full activity protocol, there is no transmission constraint imposed on the SU-Tx. Therefore, the TP is given by $p_{\text{tx}} = 1$, which means that there is no transmission delay. Substituting (13) into (8), the COP is derived as

$$\begin{aligned} p_{\text{co}} &= \mathbb{P}\left(\log\left(1+\gamma_D\right) < R_B\right) \\ &= \mathbb{P}\left(|h_{SD}|^2 < \frac{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}}{I_0 d_{SP}^{\alpha}}\,|h_{SP}|^2\right) \\ &= \frac{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}}{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}. \end{aligned} \tag{21}$$

Substituting (14) into (7), the SOP is derived as

$$\begin{aligned} p_{\text{so}} &= \mathbb{P}\left(\log_2\left(1+\gamma_E\right) > R_B - R_S\right) \\ &= \mathbb{P}\left(\log_2\left(1+\frac{I_0}{\sigma^2|h_{SP}|^2 d_{SP}^{-\alpha}} Z_{\Phi_E}\right) > R_B - R_S\right) \\ &= \mathbb{E}_{\Phi_E}\left\{1-\exp\left(-\frac{I_0 Z_{\Phi_E} d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right)\right\} \\ &= 1 - L_{Z_{\Phi_E}}\left(\frac{I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right), \end{aligned} \tag{22}$$

where $\mathbb{E}_{\Phi_E}\{\cdot\}$ denote the expectation operator over Φ_E, and $L_{Z_{\Phi_E}}(\cdot)$ denotes the Laplace transform of Z_{Φ_E}. As given in [69], $L_{Z_{\Phi_E}}(s) = \exp\left(-2\pi\lambda_E s^{2/\alpha}/\alpha\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(\frac{2}{\alpha}\right)\right)$.

Substituting (13) and (14) into (9), the TSOP is derived as

$$\begin{aligned} p_{\text{tso}} &= 1-\mathbb{P}\left(\log_2\left(1+\gamma_E\right) < R_B - R_S \;\&\; \log_2\left(1+\gamma_D\right) > R_B\right) \\ &= 1-\mathbb{P}\left(\log_2\left(1+\frac{I_0}{|h_{SP}|^2 d_{SP}^{-\alpha}}\frac{Z_{\Phi_E}}{\sigma^2}\right) < R_B - R_S \right. \\ &\qquad \left. \&\;\; \log_2\left(1+\frac{I_0}{|h_{SP}|^2 d_{SP}^{-\alpha}}\frac{|h_{SD}|^2 d_{SD}^{-\alpha}}{\sigma^2}\right) > R_B\right) \\ &= 1-\mathbb{E}_{\Phi_E}\left\{\int_{\frac{I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2} Z_{\Phi_E}}^{\infty} e^{-\left(\frac{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}}{I_0 d_{SP}^{\alpha}}+1\right)y} dy\right\} \\ &= 1-\frac{I_0 d_{SP}^{\alpha}}{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}} \\ &\qquad \times L_{Z_{\Phi_E}}\left(\frac{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right). \end{aligned} \tag{23}$$

From (21), (22) and (23), we find that p_{tso} can be also written as a function of p_{so} and p_{co}, given by

$$p_{\text{tso}} = 1-\left(1-p_{\text{co}}\right)\left(1-p_{\text{so}}\right)^{\left(1-p_{\text{co}}\right)^{-2/\alpha}}. \tag{24}$$

Note that (24) is different from (10). This verifies that the COP and the SOP are correlated for the CR network studied in this paper. Besides, we note that none of p_{co}, p_{so} and p_{tso} is controllable in the full activity protocol, since all of I_0, R_B, R_S, d_{SP} and d_{SD} are not design parameters.

B. Secrecy Guard Zone Protocol

In this protocol, the SU-Tx transmits only when there is no eavesdropper inside the secrecy guard zone. We denote the location of the SU-Tx as the origin o. Then, the secrecy guard zone around the SU-Tx with radius r is denoted by $\mathcal{B}(o,r)$. Note that the number of eavesdroppers inside $\mathcal{B}(o,r)$, denoted by N, is a Poisson random variable with mean $\pi r^2\lambda_E$. Thus, its probability mass function (PMF) is given by

$$\mathbb{P}\left(N=n\right) = \exp\left(-\pi r^2\lambda_E\right)\frac{\left(\pi r^2\lambda_E\right)^n}{n!}. \tag{25}$$

Then, the TP is derived as

$$\begin{aligned} p_{\text{tx}} &= \mathbb{P}\left(C_1 : \forall E_j \in \Phi_E, d_{SE_j} > r\right) \\ &= \mathbb{P}\left(N=0\right) \\ &= \exp\left(-\pi\lambda_E r^2\right). \end{aligned} \tag{26}$$

Substituting (15) into (8), we can obtain the COP for the secrecy guard zone protocol, which turns out to be identical to (21) and is omitted here.

Denote $\widetilde{\Phi}_E$ as the new location set of the eavesdroppers for the scenario where the transmission happens, i.e., no eavesdropper is inside the secrecy guard zone. Then, the received SNR at the eavesdropper E_{joint} for the scenario where the transmission happens is given by $\gamma_E = \frac{P}{\sigma^2}\sum_{E_j\in\widetilde{\Phi}_E}\left|h_{SE_j}\right|^2 d_{SE_j}^{-\alpha}$. Here, we define $Z_{\widetilde{\Phi}_E} = \sum_{E_j\in\widetilde{\Phi}_E}\left|h_{SE_j}\right|^2 d_{SE_j}^{-\alpha}$. Thus, the SOP for the secrecy guard zone protocol can be derived by following the same step of (22), which is given by

$$p_{\text{so}} = 1 - L_{Z_{\widetilde{\Phi}_E}}\left(\frac{I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right). \tag{27}$$

From the viewpoint of the SU-Tx, the location set, $\widetilde{\Phi}_E$, still follows a homogeneous PPP with density λ_E outside the secrecy guard zone $\mathcal{B}(o,r)$. Then, the Laplace transform of $Z_{\widetilde{\Phi}_E}$ is derived as

$$\begin{aligned} L_{Z_{\widetilde{\Phi}_E}}(s) &= \mathbb{E}_{\widetilde{\Phi}_E,\left|h_{SE_j}\right|^2}\left\{\exp\left(-s\sum_{E_j\in\widetilde{\Phi}_E}\left|h_{SE_j}\right|^2 d_{SE_j}^{-\alpha}\right)\right\} \\ &\overset{(a)}{=} \mathbb{E}_{\widetilde{\Phi}_E}\left\{\prod_{E_j\in\widetilde{\Phi}_E}\mathbb{E}_{\left|h_{SE_j}\right|^2}\left\{\exp\left(-s\left|h_{SE_j}\right|^2 d_{SE_j}^{-\alpha}\right)\right\}\right\} \\ &\overset{(b)}{=} \mathbb{E}_{\widetilde{\Phi}_E}\left\{\prod_{E_j\in\widetilde{\Phi}_E}\frac{1}{1+s d_{SE_j}^{-\alpha}}\right\} \\ &\overset{(c)}{=} \exp\left[-\lambda_E\int_{\mathbb{R}^2\setminus\mathcal{B}(o,r)}\left(1-\frac{1}{1+s x^{-\alpha}}\right)dx\right], \end{aligned} \tag{28}$$

where (a) is because of the independence between the channel gain $\left|h_{SE_j}\right|^2$ and the location of eavesdroppers, (b) follows from the exponential distribution of $\left|h_{SE_j}\right|^2$, (c) follows from the generating function of the homogeneous PPP $\widetilde{\Phi}_E$. Following from the double integral in polar coordinates, the Laplace transform $Z_{\widetilde{\Phi}_E}$ is finally given by

$$L_{Z_{\widetilde{\Phi}_E}}(s) = \exp\left(-\frac{2}{\alpha}\pi\lambda_E s^{2/\alpha}\mathrm{B}_{\left(r^{\alpha}s^{-1}+1\right)^{-1}}\left(1-\frac{2}{\alpha},\frac{2}{\alpha}\right)\right), \tag{29}$$

where $\mathrm{B}_x(p,q) = \int_0^x t^{p-1}(1-t)^{q-1}dt$ is the incomplete Beta function [70]. As such, by substituting (29) into (27),

we can derive the closed-form expression for the SOP. Since $\mathrm{B}_x(p,q)$ is an increasing function of x for any given (p,q), the Laplace transform is an increasing function of r.

Based on (15), (16) and (9), the TSOP is derived as

$$\begin{aligned} p_{\text{tso}} &= 1-\mathbb{P}\left(\log_2(1+\gamma_E)<R_B-R_S\right. \\ &\qquad \left.\&\ \log_2(1+\gamma_D)>R_B \middle| \mathbf{1}_{(C_1)}=1\right) \\ &= 1-\frac{I_0 d_{SP}^{\alpha}}{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}} \\ &\quad \times L_{Z_{\tilde{\Phi}_E}}\left(\frac{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right). \end{aligned} \tag{30}$$

From (21), (27) and (30), we note that p_{tso} for the secrecy guard zone protocol can be also written as a function of p_{so} and p_{co}, given by

$$p_{\text{tso}} = 1-(1-p_{\text{co}})\left(1-p_{\text{so}}\right)^{r_1(1-p_{\text{co}})^{-2/\alpha}}, \tag{31}$$

where

$$r_1 = \mathrm{B}_{\left(r^{\alpha}s_2^{-1}+1\right)^{-1}}\left(1-\frac{2}{\alpha},\frac{2}{\alpha}\right)\Big/\mathrm{B}_{\left(r^{\alpha}s_1^{-1}+1\right)^{-1}}\left(1-\frac{2}{\alpha},\frac{2}{\alpha}\right)$$

with

$$s_1 = I_0 d_{SP}^{\alpha}/\left(2^{R_B-R_S}-1\right)\sigma^2,$$

$$s_2 = \left(\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}\right)/\left(2^{R_B-R_S}-1\right)\sigma^2.$$

This, once again, confirms that the COP and the SOP are correlated for the CR network studied in this paper, since (31) is different from (10).

Remark 3: It can be inferred from (27) and (30) that p_{so} and p_{tso} are decreasing functions of r, since the Laplace transform is an increasing function of r. This implies that a large secrecy guard zone is beneficial for reducing the SOP and the TSOP of the secondary network. On the other hand, it can be inferred from (26) that p_{tx} is a decreasing function of r. This indicates that a large secrecy guard zone degrades the transmission delay performance. Hence, there arises a tradeoff between the security performance and the transmission delay performance incurred by the size of secrecy guard zone. Moreover, we note that the COP is still uncontrollable in this protocol, and hence having the secrecy guard zone does not help to control the reliability performance.

C. Threshold-Based Protocol

In this protocol, the SU-Tx transmits only when γ_D is larger than the predetermined threshold $\mu \in [0,\infty)$. Consequently, the TP is given by

$$\begin{aligned} p_{\text{tx}} &= \mathbb{P}\left(C_2:\gamma_D>\mu\right) \\ &= \frac{I_0 d_{SP}^{\alpha}}{\mu\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}. \end{aligned} \tag{33}$$

Note that only when $\mu \in \left[0, 2^{R_B}-1\right)$, the connection outage exists. Substituting (17) into (8), the COP for $\mu \in \left[0, 2^{R_B}-1\right)$ is derived as

$$\begin{aligned} p_{\text{co}} &= \mathbb{P}\left(\log(1+\gamma_D)<R_B \middle| \mathbf{1}_{(C_2)}=1\right) \\ &= \frac{\mathbb{P}\left(\log(1+\gamma_D)<R_B,\gamma_D>\mu\right)}{\mathbb{P}\left(\gamma_D>\mu\right)} \\ &= 1-\frac{\mu\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}. \end{aligned} \tag{34}$$

Then, the COP for $\mu \geq 0$ is given by

$$p_{\text{co}} = \begin{cases} 1-\dfrac{\mu\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}, & 0\leq\mu<2^{R_B}-1, \\ 0, & 2^{R_B}-1\leq\ \mu. \end{cases} \tag{35}$$

Substituting (18) into (7), the SOP for the threshold-based protocol is derived as

$$\begin{aligned} p_{\text{so}} &= \mathbb{P}\left(\log_2(1+\gamma_E)>R_B-R_S \middle| \mathbf{1}_{(C_2)}=1\right) \\ &= \frac{\mathbb{P}\left(\log_2(1+\gamma_E)>R_B-R_S,\gamma_D>\mu\right)}{\mathbb{P}\left(\gamma_D>\mu\right)} \\ &= \frac{\mathbb{E}_{\Phi_E}\left\{\int_0^{\frac{I_0 d_{SP}^{\alpha} Z_{\Phi_E}}{\left(2^{R_B-R_S}-1\right)N_0}}\exp\left(-\left(\frac{\mu\sigma^2 d_{SD}^{\alpha}}{I_0 d_{SP}^{\alpha}}+1\right)y\right)dy\right\}}{I_0 d_{SP}^{\alpha}/\left(\mu\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}\right)} \\ &= 1-L_{Z_{\Phi_E}}\left(\frac{\mu\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right). \end{aligned} \tag{36}$$

Substituting (17) and (18) into (9), the TSOP for this protocol is derived as (37), shown at the top of this page.

In addition, from (35) and (36), p_{tso} can be also written as a function of p_{so} and p_{co}, given by

$$p_{\text{tso}} = \begin{cases} 1-(1-p_{\text{co}})\left(1-p_{\text{so}}\right)^{(1-p_{\text{co}})^{-2/\alpha}}, & 0\leq\mu<2^{R_B}-1, \\ p_{\text{so}}, & 2^{R_B}-1\leq\mu. \end{cases} \tag{38}$$

Remark 4: In the threshold-based protocol, it is worth noting that the COP is a decreasing function of μ while the SOP is an increasing function of μ. This is due to the adaptive transmit power scheme at the SU-Tx. With such a transmit power scheme, the received SNR at the eavesdropper is probably large when the received SNR at the SU-Rx is large. Thus, the value of μ arises a tradeoff between the security performance and the reliability performance for the threshold-based protocol. Besides, we find that the TP is a decreasing function of μ, which implies that there is also a tradeoff between the transmission delay performance and the reliability performance incurred by μ.

D. Hybrid Protocol

In the hybrid protocol, the SU-Tx transmits only when there is no eavesdropper in the secrecy guard zone around the SU-Tx and the received SNR at SU-Rx is larger than the threshold μ. The TP is given by

$$\begin{aligned} p_{\text{tx}} &= \mathbb{P}\left(C_1 \& C_2 : \forall E_j \in \Phi_E, d_{SE_j}>D \text{ and } \gamma_D>\mu\right) \\ &= \frac{I_0 d_{SP}^{\alpha}}{\mu\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}\exp\left(-\pi\lambda_E D^2\right). \end{aligned} \tag{39}$$

The derivation of the COP is identical to (35) in the threshold-based protocol. Similar with the derivation of (36) and considering the effect of secrecy guard zone, the SOP for the hybrid protocol is derived as

$$p_{\text{so}} = 1-L_{Z_{\tilde{\Phi}_E}}\left(\frac{\mu\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right). \tag{40}$$

$$
\begin{aligned}
p_{\text{tso}} &= 1-\mathbb{P}\left(\log_2\left(1+\gamma_E\right)<R_B-R_S \;\&\; \log_2\left(1+\gamma_D\right)>R_B \middle| \mathbf{1}_{(C_2)}=1\right)\\
&= 1-\frac{1}{p_{\text{tx}}}\mathbb{E}_{\Phi_E}\left\{\int_{\frac{I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}Z_{\Phi_E}}^{\infty}\exp\left(-\left(\frac{\max\left\{\mu,2^{R_B}-1\right\}\sigma^2 d_{SD}^{\alpha}}{I_0 d_{SP}^{\alpha}}+1\right)y\right)dy\right\}\\
&= \begin{cases}1-\dfrac{\mu\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}L_{Z_{\Phi_E}}\left(\dfrac{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right), & 0\le\mu<2^{R_B}-1,\\ 1-L_{I_{\Phi_E}}\left(\dfrac{\mu\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right), & 2^{R_B}-1\le\mu.\end{cases}
\end{aligned}
\tag{37}
$$

$$
\begin{aligned}
p_{\text{tso}} &= 1-\mathbb{P}\left(\log_2\left(1+\gamma_E\right)<R_B-R_S \;\&\; \log_2\left(1+\gamma_D\right)>R_B \middle| \mathbf{1}_{(C_1\&C_2)}=1\right)\\
&= \begin{cases}1-\dfrac{\mu\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}L_{Z_{\tilde{\Phi}_E}}\left(\dfrac{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right), & 0<\mu<2^{R_B}-1,\\ 1-L_{Z_{\tilde{\Phi}_E}}\left(\dfrac{\mu\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right), & 2^{R_B}-1\le\mu.\end{cases}
\end{aligned}
\tag{41}
$$

Also, substituting (19) and (20) into (9), the TSOP for this protocol is given by (41), shown at the top of this page.

From (35), (40) and (41), we find that p_{tso} can be also written as a function of p_{so} and p_{co}, given by

$$
p_{\text{tso}}=\begin{cases}1-\left(1-p_{\text{co}}\right)\left(1-p_{\text{so}}\right)^{r_2\left(1-p_{\text{co}}\right)^{-2/\alpha}}, & 0\le\mu<2^{R_B}-1,\\ p_{\text{so}}, & 2^{R_B}-1\le\mu,\end{cases}
\tag{42}
$$

where

$$
r_2=\mathrm{B}_{\left(r^{\alpha}s_2^{-1}+1\right)^{-1}}\left(1-\frac{2}{\alpha},\frac{2}{\alpha}\right)\Big/\mathrm{B}_{\left(r^{\alpha}s_3^{-1}+1\right)^{-1}}\left(1-\frac{2}{\alpha},\frac{2}{\alpha}\right)
$$

with $s_3=\frac{\mu\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}$. The impact of security performance and reliability performance on the joint security and reliability performance for the hybrid protocol is mathematically characterized by (42).

VI. Secrecy Throughput Maximization

From the previous section, we find that each of r and μ plays a very important role in the performance of the transmission. Specifically, the value of r incurs a tradeoff between the security performance and the transmission delay performance. The value of μ incurs tradeoffs not only between the reliability performance and the security performance, but also between the reliability performance and the transmission delay performance.

To optimize the performance of the transmission protocols, in this section, we obtain the optimal r and/or μ that maximize the secrecy throughput subject to secrecy outage and connection outage constraints. The optimization problem is formulated as

$$
\begin{aligned}
\max_{r \text{ and/or } \mu} \quad & \eta = p_{\text{tx}}\left(1-p_{\text{to}}\right)R_S\\
\text{s. t.} \quad & p_{\text{so}}\le\varepsilon, p_{\text{co}}\le\delta, r\ge 0, \mu\ge 0,
\end{aligned}
\tag{43}
$$

where p_{tx}, p_{co}, p_{so} and p_{tso} for different protocols are derived in the previous section. When the parameter to optimize is μ, it corresponds to the threshold-based protocol; when the parameter to optimize is r, it corresponds to the secrecy guard zone protocol; when the the parameters to optimize are μ and r, it corresponds to the hybrid protocol.

In the following two subsections, we first investigate the feasible secrecy outage and connection outage constraints for each transmission protocol, under which a non-zero secrecy throughput is achievable. We then obtain the optimal solutions of r and/or μ that maximize the secrecy throughput subject to the secrecy outage and connection outage constraints. Although there is no design parameter (i.e., r or μ) to optimize for the full activity protocol, we show the feasible secrecy outage and connection outage constraints for the full activity protocol for comparison with other transmission protocols.

A. Feasibility of Constraints for Different Protocols

We denote $F\left(1\right), F\left(2\right), F\left(3\right)$ and $F\left(4\right)$ as the feasible constraints for the full activity protocol, the secrecy guard zone protocol, the threshold-based protocol and the hybrid protocol, respectively, which are detailed as follows.

$F\left(1\right)$*:* For the full activity protocol, since neither the COP nor the SOP is controllable, the security and reliability constraints are either always achievable or always not achievable. The feasible constraint range for the full activity scheme is given as a square area in the 2-D plane of ε and δ

$$
F\left(1\right)=\left\{\left(\varepsilon,\delta\right):\varepsilon_1\le\varepsilon\le 1,\delta_1\le\delta\le 1\right\},
\tag{44}
$$

where δ_1 and ε_1 denote the COP in (21) and the SOP in (22), respectively.

$F\left(2\right)$*:* For the secrecy guard zone protocol, the SOP is a decreasing function of r and $\lim\limits_{r\to\infty} p_{so}=0$, while the COP is still uncontrollable. Hence, the feasible constraint range for the secrecy guard zone protocol is given by

$$
F\left(2\right)=\left\{\left(\varepsilon,\delta\right):0<\varepsilon\le 1,\delta_1\le\delta\le 1\right\}.
\tag{45}
$$

$F\left(3\right)$*:* For the threshold-based protocol, the COP is a decreasing function of μ while the SOP is an increasing

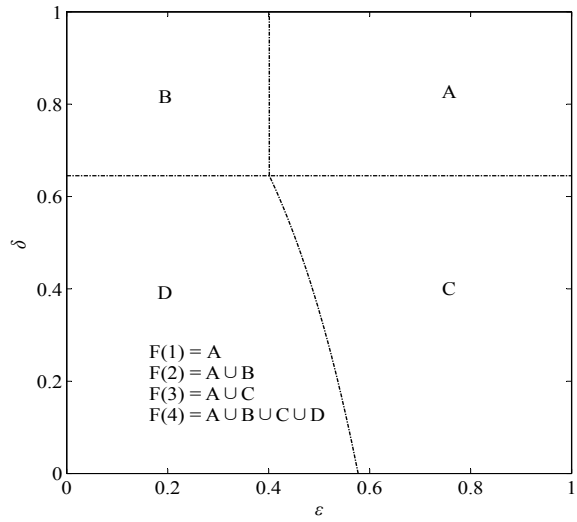


Fig. 2. An illustration of the feasible constraint region for the network with $R_B = 3$, $R_S = 1$ and $I_0/\delta^2 = 10$.

function of μ. To be specific, when $\delta \geq \delta_1$, the minimum value of ε is ε_1 since μ can be set to zero; when $\delta < \delta_1$, by setting $p_{\text{co}} = \delta$, we can obtain the minimum value of the ε as

$$\varepsilon_2 = 1 - L_{Z_{\Phi_E}}\left((1-\delta)\frac{\left(2^{R_B-1}\right)\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right). \quad (46)$$

Therefore, the feasible constraint range for the threshold-based protocol is given by

$$F(3) = \{(\varepsilon,\delta) : \max(\varepsilon_1,\varepsilon_2) \leq \varepsilon \leq 1, 0 \leq \delta \leq 1\}. \quad (47)$$

$F(4)$*:* For the hybrid protocol, through the analysis in Sections V we know that $\lim_{r\to\infty} p_{\text{so}} = 0$ and if $\mu \geq 2^{R_B-1}$, $p_{\text{co}} = 0$. So, any required reliability and security constraints are feasible by appropriately adjusting μ and r. Hence, the feasible constraint range for the hybrid protocol is given by

$$F(4) = \{(\varepsilon,\delta) : 0 < \varepsilon \leq 1, 0 \leq \delta \leq 1\}. \quad (48)$$

Figure 2 gives an example of the feasible reliability and security constraints for different protocols. The feasible constraint region for the full activity protocol is shown as the square field A in the figure. The field of A ∪ B is the feasible constraint region of the secrecy guard zone protocol. It is observed that the secrecy guard zone protocol allows a more stringent security constraint, which can arbitrarily approach zero. The feasible constraint region of the threshold-based protocol is the field of A ∪ C. As shown in the figure, the threshold-based protocol extends the reliability constraint to the $0 \leq \delta \leq 1$. Meanwhile, at field C, the feasible value of ε increases with the stringent of the reliability constraint. The feasible constraint region for the hybrid protocol is given by A ∪ B ∪ C ∪ D. The hybrid protocol extends the feasible constraint region to the whole $\varepsilon - \delta$ plane field.

B. Optimal Design

Note that when $r = 0$ and $\mu = 0$, the hybrid protocol reduces to the full activity protocol; when $\mu = 0$, the hybrid protocol reduces to the secrecy guard zone protocol; when $r = 0$, the hybrid protocol reduces to the threshold-based protocol. Thus, the hybrid protocol mathematically includes all of the other three transmission protocols as special cases. In this subsection, we show the optimal solutions for the hybrid protocol only, and the optimal solutions for the other protocols can be easily obtained accordingly.

The solution to the optimization problem for the hybrid protocol is given by the following proposition.

Proposition 1: The optimal design parameters (r^*, μ^*) of the hybrid protocol are given by

$$(r^*,\mu^*) = \begin{cases} (0,[0,\mu_{\text{UB}}]), & \text{if } \varepsilon \geq \varepsilon_1 \text{ and } \delta \geq \delta_1, \\ (g(0),0), & \text{if } 0 < \varepsilon < \varepsilon_1 \text{ and } \delta \geq \delta_1, \\ (0,[\mu_{\text{LB}},\mu_{\text{UB}}]), & \text{if } \varepsilon \geq \varepsilon_2 \text{ and } 0 \leq \delta < \delta_1, \\ (g(\mu_{\text{LB}}),\mu_{\text{LB}}), & \text{if } 0 < \varepsilon < \varepsilon_2 \text{ and } 0 \leq \delta < \delta_1, \end{cases} \quad (49)$$

where

$$g(\mu) = (\phi(\mu))^{1/\alpha}\left(\left(\text{B}^{-1}_{\frac{-\alpha\ln(1-\varepsilon)}{2\pi\lambda_E(\phi(\mu))^{1/\alpha}}}\left(1-\frac{2}{\alpha},\frac{2}{\alpha}\right)\right)^{-1}-1\right)^{1/\alpha}, \quad (50)$$

$$\mu_{\text{LB}} = (1-\delta)\left(2^{R_B}-1\right) - \frac{I_0 d_{SP}^{\alpha}}{\sigma^2 d_{SD}^{\alpha}}\delta, \quad (51)$$

$$\mu_{\text{UB}} = \min\left(2^{R_B}-1, \left(\frac{-\alpha\ln(1-\varepsilon)}{2\pi\lambda_E\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(\frac{2}{\alpha}\right)}\right)^{\alpha/2}\frac{2^{R_B-R_S}-1}{d_{SD}^{\alpha}} - \frac{I_0 d_{SP}^{\alpha}}{\sigma^2 d_{SD}^{\alpha}}\right), \quad (52)$$

with $\phi(\mu) = \frac{\mu\sigma^2 d_{SD}^{\alpha}+I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}$ and $\text{B}_x^{-1}(p,q)$ representing the inverse function of $\text{B}_x(p,q)$.

Proof: See Appendix. ■

Remark 5: The optimal r and μ vary with the security and reliability constraints. Note that the optimal values of μ are given by feasible regions for particular constraints. Specifically, if a higher reliability level is required, it is wise to set $\mu^* = \mu_{\text{UB}}$; if a higher security level is required, it is wise to set $\mu^* = \mu_{\text{LB}}$. Meanwhile, a higher security level requires a larger optimal r and confines the upper bound of μ, while a higher reliability level requires a larger lower bound of μ and a larger optimal r. We also find that with fixed security and reliability constraints, the optimal r is an increasing function of the eavesdropper density and the upper bound of μ is a decreasing function of the eavesdropper density. Furthermore, we note that η is a decreasing function of r. Therefore, secrecy throughput should be compromised (i.e., allowing a smaller value of η) in order to achieve higher security and reliability levels.

It is worth mentioning that similar secrecy guard zone protocols have been previously studied in, e.g., [12, 13, 15], and similar threshold-based protocols has been previously investigated in, e.g., [65, 71]. Different from the existing secrecy guard zone protocols in [12, 13, 15], our proposed secrecy guard zone protocol is applicable in the CR network where the

SU-Tx has an adaptive transmit power. Most importantly, none of [12, 13, 15] has studied the optimal design of the secrecy guard zone. In contrast, we have derived the optimal radius of the guard zone that maximizes the secrecy throughput. Note that the optimal design of the radius is very important for the performance of the secrecy guard zone protocol. Different from the existing threshold-based protocols in [65, 71], our proposed threshold-based protocol is specifically designed for the CR network where the SU-Tx has an adaptive transmit power. The consideration of adaptive transmit power at the SU-Tx protects the primary network from interference by ensuring a low interference power received at the primary user. We have derived the optimal design of the threshold value, which is dependent on the conditions of both the channel from SU-Tx to PU-Rx and the channel from SU-Tx to SU-Rx. Although the optimal SNR threshold has also been designed in [65], the result in [65] cannot be applied in the secure CR network. In [65], the transmit power is simply a fixed value without the consideration of protecting the primary network from interference. Actually, the consideration of adaptive transmit power in this paper makes the derivation of optimal SNR threshold much more complicated.

VII. Numerical Results and Discussion

In this section, we first present and compare the numerical results for different transmission protocols. Then, we show the interaction of different design parameters and their effects on the reliability and security performance. Finally, we present numerical results of the secrecy throughput to illustratively show the performance improvement by the optimal design parameters. The results shown in this section are all for the network with $\alpha = 4$, $I_0/\sigma^2 = 10$ dB, $R_B = 3$, $R_S = 1$, $d_{SD} = 5$ and $d_{SP} = 5$.

We first compare the SOP and the COP of different transmission protocols. Figure 3 plots the SOP, p_{so}, and the COP, p_{co}, versus the eavesdropper density, λ_E. We note that as λ_E increases, p_{so} keeps increasing and p_{co} remains constant. Compared with the full activity protocol, the secrecy guard zone protocol significantly decreases SOP while never alters COP. The threshold-based protocol decreases COP while increases SOP. This finding is different from the results for non-cognitive networks [65] and [66], in which introducing the SNR threshold does not increase the p_{so}. As explained previously in Section V, such a finding is due to the adaptive transmit power adopted at the SU-Tx. In addition, these observations can help the designers of real CR networks to appropriately select the transmission protocol according to the importance of different requirements. For example if the real network has a stringent requirement on the reliability performance, it is preferable to adopt the threshold-based protocol by ensuring the one-bit feedback from the SU-Rx to SU-Tx. Taking the advantages of the secrecy guard zone protocol and the threshold-based protocol, the hybrid protocol can decrease both SOP and COP compared with the full activity protocol.

We then compare the TSOP of different transmission protocols. Figure 4 plots the TSOP, p_{tso}, versus the eavesdropper density, λ_E. From the figure, we find that p_{tso} is an increasing

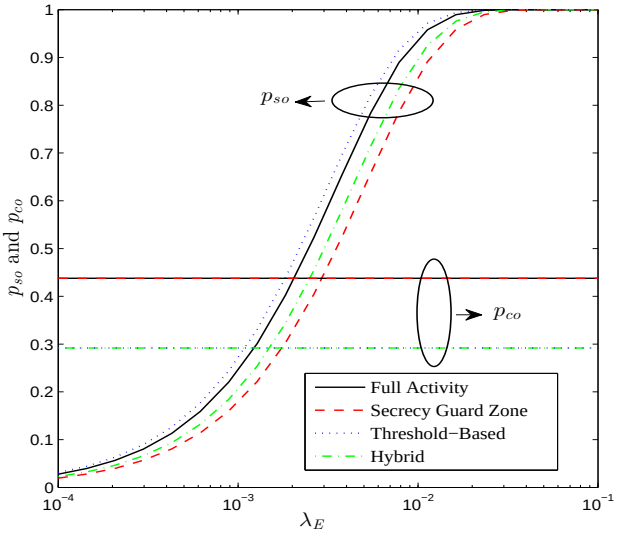


Fig. 3. SOP and COP versus the eavesdropper density for different transmission protocols.

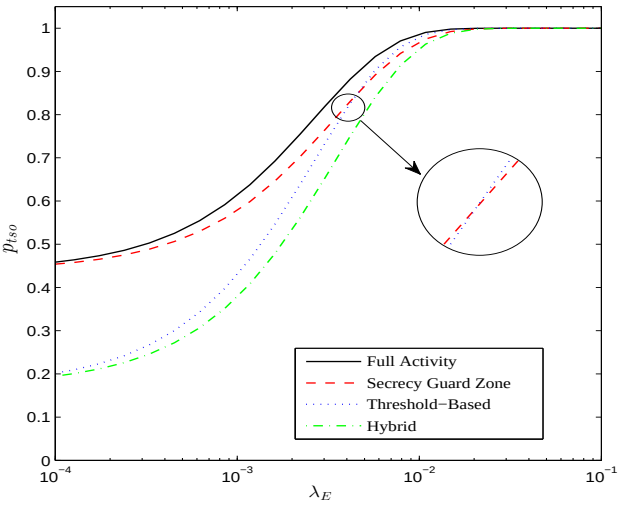


Fig. 4. TSOP versus the eavesdropper density for different transmission protocols.

function of λ_E. As the reference, the full activity protocol has the worst TSOP. The hybrid protocol performs the best. In addition, when the eavesdropper density is low, the threshold-based protocol outperforms the secrecy guard zone protocol. On the contrary, the secrecy guard zone protocol outperforms the threshold-based protocol, when the eavesdropper density is high.

In the following, we present the impact of the SNR threshold, μ, and the secrecy guard zone radius, r, on the network performance by Figures 5, 6 and 7. Figure 5 plots p_{tx}, p_{co}, p_{so} and p_{tso}, versus the SNR-threshold, μ. As the figure shows, p_{co} is a decreasing function of μ, and it is equal to zero when $\mu \geq 2^{R_B} - 1$. The p_{so} is an increasing function of μ and p_{tx} is a decreasing function of μ. These observations imply that a larger SNR-threshold can enhance the reliability performance

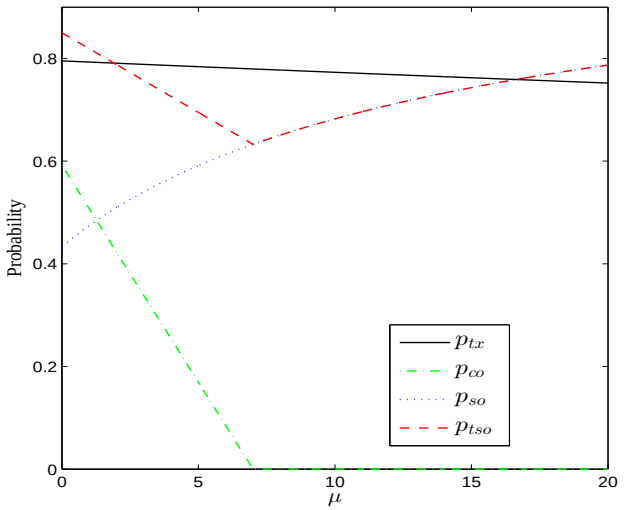


Fig. 5. TP, COP, SOP and TSOP versus the SNR threshold with eavesdropper density $\lambda_E = 10^{-3}$.

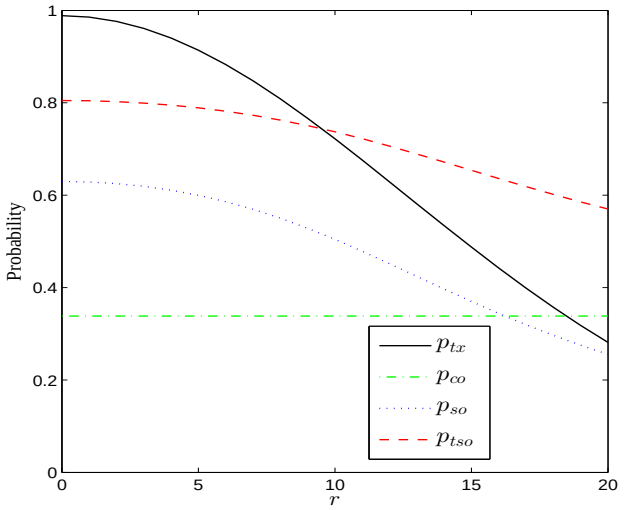


Fig. 6. TP, COP, SOP and TSOP versus the radius of the secrecy guard zone with eavesdropper density $\lambda_E = 10^{-3}$.

while harm the security performance and the transmission delay performance. Consequently, p_{tso}, which characterizes the joint performance of reliability and security, is not a monotonous function of μ. The p_{tso} firstly decreases and then increases as μ increases, and p_{tso} is minimized at $\mu = 2^{R_B} - 1$. According to these observations, the designers of real CR networks can wisely set up the SNR threshold to balance the tradeoff among the delay, reliability and secrecy performances of the network. Figure 6 plots the p_{tx}, p_{co}, p_{so} and p_{tso} versus the radius of the secrecy guard zone, r. As shown in the figure, both of p_{so} and p_{tx} are decreasing functions of r. This implies that a high security level is achieved at the cost of a large transmission delay. Thus, a large radius of the secrecy guard zone is not always beneficial for real CR networks. In addition, we find that COP remains constraint with the increase of the

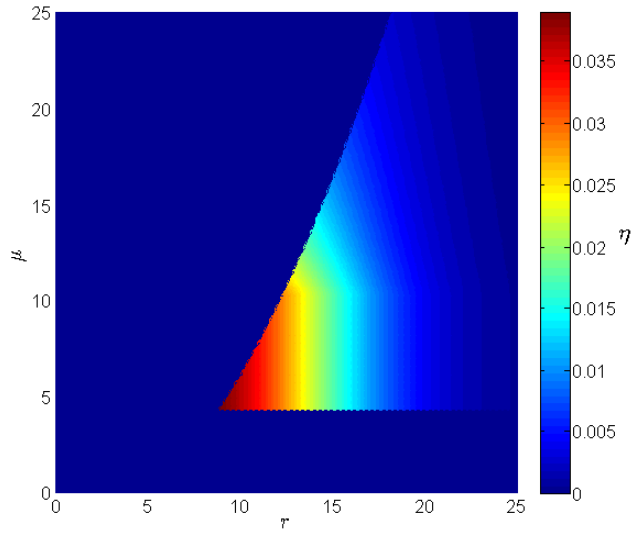


Fig. 7. The secrecy throughput versus secrecy guard radius r and the SNR-threshold μ with eavesdropper density $\lambda_E = 10^{-3}$. The security and reliability constraints are set as $\varepsilon = 0.4$, $\delta = 0.4$

radius, since the COP is not related to the radius. Figure 7 plots the secrecy throughput, η, against μ and r. In the contour plot, the values of the secrecy throughput from low to high are represented by different colors from blue to red. The security constraint is set as $\delta = 0.4 < \delta_1$ and the reliability constraint is set as $\varepsilon = 0.4 < \max(\varepsilon_1, \varepsilon_2)$ from Figure 2. As shown in the figure, the non-zero secrecy throughput can be achieved with proper designs of μ and r for the given network. While, improper designs of μ and r will result in the zero secrecy throughput of the transmission. These observations directly present the importance of SNR threshold and secrecy guard zone radius on the achievable secrecy throughput of real CR networks. In addition, we find that there exists an optimal pair of (r, μ) maximizing the secrecy throughput. From Proposition 1, we obtain that the optimal pair of (r, μ) for the given network is $(r^*, \mu^*) = (8.85, 4.35)$, which is consistent with the results shown in the figure.

Finally, we compare the achievable secrecy throughput for different transmission protocols versus the security constraint, ε, and the reliability constraint, δ, by Figure 8. As shown in the figure, the secrecy guard zone protocol can achieve the non-zero secrecy throughput under more stringent security constraint, compared with the full activity protocol. The threshold-based protocol can achieve the non-zero secrecy throughput under more stringent reliability constraint, compared with the full activity protocol. We also note that for the threshold-based protocol, the security level has to be compromised to achieve the non-zero secrecy throughput as the reliability constraint becomes stricter. In addition, compared with the other three protocols, the hybrid protocol can achieve the non-zero secrecy throughput under the most stringent security and reliability constraints. Therefore, we can summarize the wise choices of different transmission protocols under different conditions as follows. When both the security and the reliability constraints are very loose, it is wise to adopt the full activity protocol

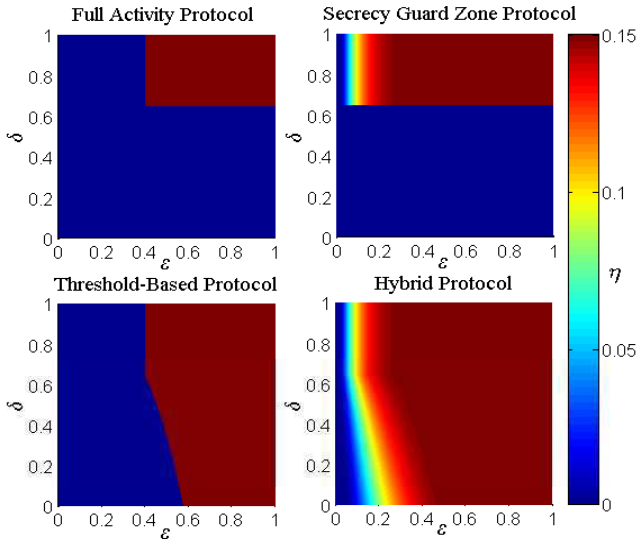


Fig. 8. The optimized secrecy throughput η for different transmission protocols as a function of the security constraint ε and the reliability constraint δ with eavesdropper density $\lambda_E = 10^{-3}$.

due to its simple mechanism. When the security constraint is stringent but the reliability constraint is loose, it is preferable to adopt the secrecy guard zone protocol. When the reliability constraint is stringent but the security constraint is loose, it is preferable to adopt the threshold-based protocol. When both the security and the reliability constraints are stringent, it is wise to adopt the hybrid protocol.

VIII. Conclusion

In this paper, we studied the secure communication in an underlay CR networks with multiple movable eavesdroppers with a HPPP location entity at each snapshot of time. Importantly, the location set of eavesdroppers is assumed unknown at the legitimate side. We considered the scenario where the SU-Tx sends confidential messages to the SU-Rx with an instantaneous power constraint in order not to interfere the PU. To achieve physical layer security in such a CR network, we proposed four transmission protocols according to different assumptions on the channel knowledge at SU-Tx and the location knowledge about the eavesdroppers. We comprehensively analyzed and compared the security, reliability, transmission delay and overall performance for different transmission protocols. Moreover, we optimized the design parameters (r and/or μ) to maximize the secrecy throughput for the proposed transmission protocols. Our results showed that the secrecy guard zone protocol can improve security performance while the threshold-based protocol can improve the reliability performance, and the hybrid protocol can achieve the best overall performance.

In this paper, we assumed that the encoding rates at the transmitter are fixed, and hence are not design parameters. One interesting future research direction is to investigate the scenario where the encoding rates can be designed. This will give more degrees of freedom for the transmission design. We can further analyze the benefits brought by the design of encoding rates by comparing the achievable secrecy throughput in such a scenario and the achievable secrecy throughput in this work. Another interesting research direction is to investigate the practical scenario where the CSI is imperfectly known at the receiver side. This paper assumed that the perfect CSI is available at the receiver, while the channel estimation at the receiver is often not error-free in practice. Thus, it is interesting to study the impact of having imperfect CSI at the receiver on the design of secure CR networks.

Appendix

Proof of Proposition 1

We first determine the dependence of η on r and μ. Substituting (39) and (41) into (11), the secrecy throughput η can be derived as

$$\eta = \frac{I_0 d_{SP}^{\alpha} \exp\left(-\pi\lambda_E r^2\right)}{\max\left\{2^{R_B}-1,\mu\right\}\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}} \times L_{Z_{\tilde{\Phi}_E}}\left(\frac{\max\left\{2^{R_B}-1,\mu\right\}\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right) R_S. \tag{53}$$

Taking first-order derivative of η with respect to r, we obtain

$$\frac{\partial \eta(r,\mu)}{\partial r} = -2\pi\lambda_E r\left(1-\left(r^{\alpha}\omega^{-1}+1\right)^{-1}\right)\eta < 0, \tag{54}$$

where $\omega = \frac{\max\left\{\mu, 2^{R_B}-1\right\}\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}{\sigma^2\left(2^{R_B-R_S}-1\right)}$. This implies that the secrecy throughput is a decreasing function of radius, r. In addition, from (53) we find that when $\mu > 2^{R_B}-1$, η is a decreasing function of μ and when $\mu \leq 2^{R_B}-1$, η remains constant. Therefore, it is wise to have $\mu \leq 2^{R_B}-1$.

In the following, we derive the optimal values of r and μ for different ranges of security and reliability constraints.

Case 1: $\delta \geq \delta_1$ and $\varepsilon \geq \varepsilon_1$, shown as the field A in Figure 2. In this case, since security constraint is loose enough and η is a decreasing function of r, it is optimal to set $r = 0$. The lower bound of μ is equal to zero due to the loose reliability constraint. In addition, to satisfy the security constraint, there is an upper bound of μ. By solving $p_{\text{so}} = \varepsilon$ and according to $\mu \leq 2^{R_B}-1$, we derive the upper bound as (52). Thus, the optimal values of r and μ for this case is given by

$$(r^*, \mu^*) = (0, [0, \mu_{UB}]). \tag{55}$$

Case 2: $\delta \geq \delta_1$ and $0 < \varepsilon < \varepsilon_1$, shown as the field B in Figure 2. In this case, the reliability constraint is loose enough while the security constraint is stringent. To satisfy the security constraint, there is a lower bound of r. By solving $p_{\text{so}} = \varepsilon$, we derive the lower bound as (50). From (50), we know that $g(\mu)$ is an increasing function of μ. Since $\delta \geq \delta_1$, it is optimal to minimize μ to zero. Therefore, the optimal values of r and μ for this case is given by

$$(r^*, \mu^*) = (g(0), 0). \tag{56}$$

Case 3: $0 \leq \delta < \delta_1$ and $\varepsilon \geq \varepsilon_2$, shown as the field C in Figure 2. In this case, the security constraint is loose enough while the reliability constraint is stringent. To satisfy the reliability constraint, there is a lower bound of μ. By solving $p_{\text{co}} = \delta$, we derive the lower bound as (51). Same to Case 1, there is also an upper bound of μ given by (52) to

satisfy the security constraint. Therefore, the optimal values of r and μ for this case is given by

$$(r^*, \mu^*) = (0, [\mu_{\rm LB}, \mu_{\rm UB}]) . \quad (57)$$

Case 4: $0 < \varepsilon < \varepsilon_2$ and $0 \leq \delta < \delta_1$, shown as the field D in Figure 2. In this case, both the reliability and the security constraints are stringent. To satisfy the reliability constraint, there is a lower bound of μ given by (51). Same to the Case 2, there is a lower bound of r given by (50). Since $g(\mu)$ is an increasing function of μ, it is optimal to minimize μ to $\mu_{\rm LB}$. Hence, the optimal values of r and μ for this case is given by

$$(r^*, \mu^*) = (g(\mu_{\rm LB}), \mu_{\rm LB}) . \quad (58)$$

Finally, the the optimal values of r and μ for different constraint ranges are summarized by Proposition 1.

REFERENCES

[1] J. Mitola and G. Q. Maguire, "Cognitve radio: Making software radios more personal," *IEEE Personal Commun.*, vol. 6, no. 4, pp. 13–18, Apr. 1999.

[2] Y. T. Hou, A. Wyglinski, M. Nekove, H. Zhang, R. Chandramouli, and F. Martin, "Guest editorial: Special issue on cognitive radio oriented wireless networks and communications," *Moble. Netw. Appl.*, vol. 13, no. 5, pp. 411–415, May 2008.

[3] Y. Zou, Y.-D. Yao, and B. Zheng, "Cooperative relay techniques for cognitive radio systems: Spectrum sensing and secondary user transmissions," *IEEE Commun. Mag.*, vol. 50, no. 4, pp. 98–103, Apr. 2012.

[4] Y.-C. Liang, Y. Zeng, E. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 50, no. 4, pp. 98–103, Apr. 2012.

[5] H. Li, "Cooperative spectrum sensing via belief propagation in specrum-heterogeneous cognitive radio systems," in *Proc. IEEE Wireless Commun. and Netw. Conf. (WCNC)*, Sydney, Australia, Apr. 2010, pp. 1–6.

[6] R. Zhang and Y.-C. Liang, "Exploiting multi-antennas for opportunistic spectrum sharing in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 88–102, Feb. 2008.

[7] Y. Zou, J. Zhu, B. Zheng, and Y.-D. Yao, "An adaptive cooperation diversity scheme with best-relay selection in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 58, no. 10, pp. 5438–5445, Oct. 2010.

[8] H. Wen, X. Zhu, and L. Zhou, "A framework of the PHY-layer approach to defense against security threats in cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 34–39, Mar. 2013.

[9] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.

[10] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2013.

[11] M. Bloch and J. Barros, *Physical Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[12] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks – Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[13] ——, "Secure communication in stochastic wireless networks – Part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.

[14] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "Modeling location uncertainty for eavesdroppers: A secrecy graph approach," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Austin, TX, June 2010, pp. 2627–2631.

[15] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[16] M. Bloch, J. Barros, M. Rodrigues, and S. Mclaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[17] A. Ghasemi and E. S. Sousa, "Fundamental limits of spectrum-sharing in fading environments," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 649–658, Feb. 2007.

[18] L. Musavian and S. Aissa, "Capacity and power allocation for spectrum sharing communications in fading channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 1, pp. 148–156, Jan. 2009.

[19] L. Luo, Z. Ping, G. Zhang, and J. Qin, "Outage performance for cognitive relay networks with underlay spectrum sharing," *IEEE Commun. Lett.*, vol. 15, no. 7, pp. 710–712, July 2011.

[20] T. Jiang, H. Wang, and A. V. Vasilakos, "QoE-driven channel allocation schemes for multimedia transmission of priority-based secondary users over cognitive radio networks," *IEEE J. Sel. Areas in Commun.*, vol. 30, no. 7, pp. 1215–1224, Aug. 2012.

[21] S.-S. Byun, I. Balashingham, A. V. Vasilakos, and H.-N. Lee, "Computation of an equilibrium in spectrum markets for cognitive radio networks," *IEEE Trans. Comput.*, vol. 63, no. 2, pp. 304–316, Feb. 2014.

[22] V. Chakravarthy, X. Li, Z. Wu, M. A. Temple, F. Garber, R. Kannan, and A. V. Vasilakos, "Novel overlay/underlay cognitive radio waveforms using SD-SMSE framework to enhance spectrum efficiency-part I: theoretical framework and analysis in AWGN channel," *IEEE Trans. Commun.*, vol. 57, no. 12, pp. 3794–3804, Dec. 2009.

[23] D. Lopez-Perez, X. Chu, A. V. Vasilakos, and H. Claussen, "On distributed and coordinated resource allocation for interference mitigation in self-organizing lte networks," *IEEE/ACM Trans. Netw.*, vol. 21, no. 4, pp. 1145–1158, Aug. 2013.

[24] Z. Wang and W. Zhang, "Opportunistic spectrum sharing with limited feedback in poisson cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 7098–7109, Dec. 2014.

[25] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Achieving cognitive and secure transmissions using multiple antennas," in *Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Commun. (PIMRC)*, Singapore, Sep. 2009, pp. 1–5.

[26] ——, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wirel. Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[27] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas in Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.

[28] M. Youssef and M. L. C. V. A. V. Ibrahim, M. Abdelatif, "Routing metrics of cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 92–109, Mar. 2014.

[29] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, "A survey of security challenges in cognitive radio networks: solutions and future research directions," *Proc. IEEE*, vol. 100, no. 12, pp. 3172–3186, Dec. 2012.

[30] X. Guan, Y. Cai, and W. Yang, "Increasing secrecy capacity via joint design of cooperative beamforming and jamming," in *Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Commun. (PIMRC)*, Toronto, Sep. 2011, pp. 1274–1278.

[31] C. Wang and H. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1814–1827, Nov. 2014.

[32] F. Gabry, A. Zappone, R. Thobaben, E. Jorswieck, and M. Skoglund, "Energy efficiency analysis of cooperative jamming in cognitive radio networks with secrecy constraints," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 437–440, Aug. 2015.

[33] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

[34] H. Sakran, M. Shokair, O. Nasr, S. EI-Rabaie, and A. A. EI-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676–2687, 2012.

[35] M. Haenggi, J. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, p. 1029C1046, Sep. 2012.

[36] B. B. l. F. Baccelli and P. Miihlethaler, "Stochastic analysis of spatial and opportunistic ALOHA," *IEEE J. Select. Areas Commun.*, vol. 27, no. 7, pp. 1105–1119, Sep. 2009.

[37] S. Weber and J. G. Andrews, *Transmission Capacity of Wireless Networks*, 1st ed. Hanover, MA: Now Publishers Inc., 2012.

[38] S. Srinivasa and M. Haenggi, "Distance distributions in finite uniformly random networks: Theory and applications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 940–949, Feb. 2010.

[39] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inform. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[40] Y. Liang, H. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE Int. Symp. on Information Theory (ISIT)*, Seoul, Korea, June 2009, pp. 1189–1193.

[41] C. Capar, B. L. D. Goeckel, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *Proc. IEEE Int. Conf. on Computer Commun. (INFOCOM)*, Orlando, USA, Mar. 2012, pp. 1152–1160.

[42] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28–33, Mar. 2013.

[43] Y. Q. Z. Shu, Y. L. Yang and R. Q. Hu, "Impact of interference on secrecy capacity in a cognitive radio network," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Houston, TX, USA, Dec. 2011, pp. 1–6.

[44] B. Liu, J. Bi, and A. V. Vasilakos, "Toward incentivizing anti-spoofing deployment," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 3, pp. 436–450, Mar. 2014.

[45] W. Tao, L. Yao, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, pp. 1–12, Mar. 2015.

[46] H. Yang, Y. Zhang, Y. Zhou, X. Fu, H. Liu, and A. V. Vasilakos, "Provably secure three-party authenticated key agreement protocol using smart cards," *Computer Networks*, vol. 58, 2014.

[47] M. Yang, Y. Li, D. Jin, L. Zeng, X. Wu, and A. V. Athanasios, "Software-defined and virtualized future mobile and wireless networks: a survey," *Moble. Netw. Appl.*, vol. 20, no. 1, pp. 4–18, Jan. 2014.

[48] Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and softwargfined networking," *Security and Communication Networks*, Mar. 2015.

[49] M. A. Khan, H. Tembine, and A. V. Vasilakos, "Game dynamics and cost of learning in heterogeneous 4G networks," *IEEE J. Sel. Areas in Commun.*, vol. 30, no. 1, pp. 198–213, Jan. 2012.

[50] D. Lopez-Perez, X. Chu, A. V. Vasilakos, and H. Claussen, "Power minimization based resource allocation for interference mitigation in OFDMA femtocell networks," *IEEE J. Sel. Areas in Commun.*, vol. 32, no. 2, pp. 333–344, Feb. 2014.

[51] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014.

[52] P. Li, S. Guo, S. Yu, and A. V. Vasilakos, "Codepipe: An opportunistic feeding and routing protocol for reliable multicast with pipelined network coding," in *Proc. IEEE Int. Conf. on Computer Communications (Inforcom)*, Orlando, FL, USA, Mar. 2012, pp. 100–108.

[53] M. Chen, J. Wan, S. Gonzalez, X. Liao, and V. C. M. Leung, "A survey of recent developments in home M2M networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 98–114, Mar. 2014.

[54] A. Afzal, M. Z. S. S. A. R. Zaidi, M. A. Imran, M. Ghogho, A. V. Vasilakos, D. C. McLernon, and K. Qaraqe, "The cognitive internet of things: A unified perspective," *Moble. Netw. Appl.*, vol. 20, no. 1, pp. 72–85, Jan. 2015.

[55] J. Qi, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, Aug. 2014.

[56] D. Wu, J. Wang, R. Q. Hu, Y. Cai, and L. Zhou, "Energy-efficient resource sharing for mobile device-to-device multimedia communications," *IEEE Trans. Veh. Technol.*, vol. 63, no. 5, pp. 2093–2103, Jun. 2014.

[57] M. Haenggi and R. K. Ganti, *Interference in Large Wireless Networks*, 1st ed. Hanover, MA: Now Publishers Inc., 2009.

[58] B. B. l. F. Baccelli and P. Muhlethaler, "An aloha protocol for multihop mobile wireless networks," *IEEE Trans. Inform. Theory*, vol. 52, no. 2, pp. 421–436, Feb. 2006.

[59] X. Yang and A. P. Petropulu, "Co-channel interference modeling and analysis in a poisson field of interferers in wireless communications," *IEEE Trans. Signal Processing*, vol. 51, no. 1, pp. 64–76, Jan. 2003.

[60] J. Lee, H. Wang, J. G. Andrews, and D. Hong, "Outage probability of cognitive relay networks with interference constraints," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 390–395, Feb. 2011.

[61] F. Rafael, V. Guimaraes, D. B. da Costa, T. A. Tsiftsis, C. C. Cavalcante, and G. K. Karagiannidis, "Multiuser and multirelay cognitive radio networks under spectrum sharing constraints," *IEEE Trans. Vel. Technol.*, vol. 63, no. 1, pp. 433–439, Jan. 2014.

[62] R. Etkin, A. Parekh, and D. Tse, "Spectrum sharing for unlicensed bands," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 2, pp. 517–428, Apr. 2007.

[63] L. Musavian, S. Aïssa, and S. Lambotharan, "Effective capacity for interference and delay constrained cognitive-radio relay channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 5, pp. 1698–1707, May 2010.

[64] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[65] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[66] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.

[67] X. Tang, R. Liu, and P. Spasojević, "On the throughput of secure hybrid-ARQ protocols for gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Mar. 2010.

[68] A. Hasan and J. G. Andrews, "The guard zone in wireless ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 3, pp. 897–906, Mar. 2013.

[69] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When does relay transmission give a more secure connection in wireless ad hoc networks?" *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 624–632, Apr. 2014.

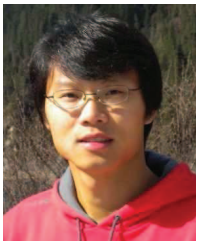
[70] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, 7th ed. Academic Press, 2007.

[71] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

Xiaoming Xu (S'13) received the B.S. degree in communication engineering from College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2011. He is currently pursuing the Ph.D. degree in communications and information system in College of Communications Engineering, PLA University of Science and Technology. His research interests include stochastic geometry, cooperative communications, and physical-layer security of wireless communications.

Biao He (S'13) received the B.E. (hons.) degree in electronic and communication systems from the Australian National University (ANU) in 2012. At the same year, he received the B.E. degree in information engineering from Beijing Institute of Technology (BIT). Currently, he is pursuing his Ph.D. degree in the Research School of Engineering at the ANU. His research interests include physical layer security, wireless communications, and information theory.

Weiwei Yang (S'08-M'12) received the B.S., M.S., and Ph.D. degrees from College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2003, 2006, and 2011, respectively. His research interests include orthogonal frequency domain multiplexing systems, signal processing in communications, cooperative communications, wireless sensor networks and network security.



Xiangyun Zhou (M'11) received the B.E. (hons.) degree in electronics and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the Australian National University in 2007 and 2010, respectively. From 2010 to 2011, he worked as a postdoctoral fellow at UNIK - University Graduate Center, University of Oslo, Norway. He joined the Australian National University in 2011 and currently works as a Senior Lecturer. His research interests are in the fields of communication theory and wireless networks.

Dr. Zhou currently serves on the editorial board of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE COMMUNICATIONS LETTERS. He also served as a guest editor for IEEE COMMUNICATIONS MAGAZINE's feature topic on wireless physical layer security in 2015 and EURASIP Journal on Wireless Communications and Networking's special issue on energy harvesting wireless communications in 2014. He is a co-chair of the ICC workshop on wireless physical layer security at ICC'14, ICC'15 and ICC'16. He also chairs the special interest group on energy harvesting communication networks under the IEEE technical committee on green communications & computing since 2015. He was the chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society from 2013 to 2014. He is a recipient of the Best Paper Award at ICC'11.

Yueming Cai (M'05–SM'12) received his B.S. degree in Physics from Xiamen University, Xiamen, China in 1982, the M.S. degree in Micro-electronics Engineering and the Ph.D. degree in Communications and Information Systems both from Southeast University, Nanjing, China in 1988 and 1996, respectively. His current research interests include MIMO systems, OFDM systems, signal processing in communications, cooperative communications and wireless sensor networks.